STATE OF MICHIGAN
Family Independence Agency

Suite 1112 Grand Tower Bldg.
235 S. Grand Ave.
P.O. Box 30037
Lansing, MI 48909
www.mfia.state.mi.us

Office of Internal Audit

Tel: 517 373-8770
Fax: 517 373-8771

Memo

To: David Mork, Director
Michigan State Disbursement Unit

Date: January 26, 2004

From: Rita Barker, Director
Office of Internal Audit

Subject: Michigan State Disbursement Unit SAS 70 Audit Report Review
Project 2004-056

The Office of Internal Audit performed a limited scope review of the most recent SAS 70 Audit Report, covering control policies and procedures placed in operation for the period October 1, 2002-September 30, 2003, at the Michigan State Disbursement Unit (MiSDU). Objectives of our review were:

1. To determine if the annual MiSDU SAS 70 report provides adequate control environment coverage

2. Provide recommendations to MiSDU management if control environment coverage can be improved

The scope of our review included obtaining and reading the most recent MiSDU SAS 70 reports, Internet research on what should be included in a SAS 70 audit, review and comparison of other FIA 3rd party SAS 70 audit reports, and review of State of Michigan Office of the Auditor General work papers related to information system controls at the State Disbursement Unit. We compared the control areas covered in the most recent MiSDU SAS 70 audit report with audit reports of other FIA 3rd party vendors and external research criteria.

In our opinion the MiSDU SAS 70 Report generally provides adequate coverage of the business process control environment and activities, but does not provide adequate coverage of the information system processing control environment and activities.

The information systems used by the vendor, ACS State and Local Solutions, Inc. (ACS) play an integral part in the collection and disbursement of child support payments. Therefore, in our opinion, the information system processing control environment should receive appropriate coverage in the annual MiSDU SAS 70 audit report to provide FIA assurance that the 3rd party vendor's controls at the MiSDU are in place and functioning adequately.

We provided recommendations that we feel will improve the adequacy of coverage of the information system processing control environment and activities in the next annual SAS 70 report of the MiSDU. However, since the SAS 70 audit is performed to provide assurance to clients of ACS, it is ultimately the responsibility of ACS and MiSDU Management to determine the objectives and extent of what should be included in the report.

SUMMARY LEVEL RECOMMENDATIONS

- MiSDU SAS 70 report should include a more complete and detailed description of the external parties (e.g. Bank One, ADP Print Services, PRWT, MiCSES, etc.) and non-local parties (e.g. Tarrytown Data Warehouse) affecting the MiSDU processing and control environment

- MiSDU SAS 70 report should describe the information systems used in collecting and disbursing child support payments

- Control objectives of the annual MiSDU SAS 70 audit should be modified to ensure information system control activities are covered adequately including the following control areas:
  -Internal risk assessment processes
  -Information and Communication Processes
  -Performance Monitoring Processes
  -Physical and environmental security of computer room
  -Network Controls
  -System and Data Change Management
  -Computer Operations

Detail of the above recommendations follows.

DETAILED RECOMMENDATIONS

1. Control Environment Description

We recommend that ACS Management require the independent accounting firm conducting the SAS 70 audit to include a more complete and detailed description of the external and non-local parties affecting the MiSDU processing and control environment. This description should include an overview of external parties (e.g. Bank One, ADP Print Services, PRWT, MiCSES) and ACS non-local parties (e.g. Tarrytown Data Warehouse), the extent of services they perform for ACS, and how they directly interact with MiSDU in child support payment processing.

In addition, we recommend that flowcharts of the information system processing environment at MiSDU and how it interacts with ACS central warehouse and external parties (e.g. Bank One, ADP Print Services, MiCSES, etc.) be included either in the report or as “Other Information”.

Information regarding these external and non-local parties may include:

-Description of the organizations
-Where they are located
-Services they perform for, on behalf of, or in conjunction with ACS
-How they interact with ACS
-Files and data shared between the entities
-Flowcharts of how they interact with the SDU
-Brief description of the control environment at these organizations (for example, Bank One complies with industry standards for electronic funds transfer and data privacy and has an annual audit performed over its control environment)

2. Description of Information Systems

We recommend that ACS Management require the independent accounting firm conducting the SAS 70 audit to describe the information systems used in collecting and disbursing child support payments.

The information systems used by the vendor, ACS State and Local Solutions, Inc. (ACS) play an integral part in the collection and disbursement of child support payments. A thorough description of the functionality and processes performed by the information systems would help provide a more complete picture of the overall control environment. ACS uses several information systems in the collection and disbursement of child support payments including:

Transaction Management System (TMS)
Automated Centralized Collection Receipt and Deposit System (ACCoRD)
Document Image Retrieval Online Network (DIRON)
Web-Chek
Onyx

A complete description of these information systems and a flowchart showing how they interact would greatly enhance the reader's understanding of the overall control environment in place at the MiSDU.

3. Information Systems Control Environment and Activities

We recommend that ACS Management modify the control objectives of the annual MiSDU SAS 70 audit to ensure information system control activities are covered adequately including the following control areas:

Internal risk assessment processes:
Risk assessment processes are used to identify and manage risks that could affect the vendor's ability to provide reliable child support collection and distribution processing. Risk assessment typically requires management to identify significant risks to their operations and implement appropriate measures to address these risks. Risk management can be accomplished through formal risk assessment processes such as a control self-assessment, quality assurance functions, individual information systems risk assessment, or business process functions. Additionally, it can be accomplished through less formal processes such as management discussions, management meetings, or employee feedback/input. Risk assessment processes and controls do not appear to be covered in any depth in the most recent MiSDU SAS 70 report.

Information and Communication Processes:
Information and communication processes are the methods used by management to disseminate employee and user roles and responsibilities related to transaction processing and controls, training, information systems usage and functionality, and other communication to employees and recipients. These methods may include policies and procedures, orientation and training programs, information systems, memos, e-mail, Intranet, management reports, or other correspondence mechanisms. Information and communication processes and controls do not appear to be covered in any depth in the most recent MiSDU SAS 70 report.

Performance Monitoring Processes:
Performance monitoring processes may include establishing and monitoring key business performance measures, information system performance measures, and network performance, and also may include establishing the reporting mechanisms and management reporting tools necessary to manage these processes. Performance monitoring processes and controls do not appear to be covered in any depth in the most recent MiSDU SAS 70 report.

Physical and environmental security of computer room:
Physical security controls related to the computer room may include maintaining current policies, procedures, and standards; location of the room; access by authorized personnel to the facility, computer room, servers or host computers, and consoles; and ensuring wiring and router closets are secured, etc. Environmental security controls related to the computer room may include consideration of hazards to the computer room such as water and fire detection and prevention, climate control, emergency alarms and lighting, uninteruptible power supply, and backup generators, etc. Some controls over physical security of the facility, such as access to different areas within the facility through card readers, security camera monitoring, and visitor access procedures, have been reviewed in the most recent MiSDU SAS 70 report. Including a review of physical security over the computer room would strengthen physical security control environment coverage. Environmental security controls related to the computer room do not appear to be addressed in the most recent report.

Network Controls:
Local area network (LAN) controls typically include, but are not limited to, adequate standards and procedures for implementation, configuration, administration, and maintenance of the network, granting and monitoring access to network resources, directories, and files, remote access policies and procedures, network performance monitoring, and network backup and recovery. LAN controls do not appear to be covered in the most recent MiSDU SAS 70 report.

System, Program, and Data Change Management:
Controls over changes to system files and program files may include: Establishing an adequate separation of duties between end-users, programmers, and system administration/operations; establishing written change control standards that address physical security, logical security, testing requirements and documentation, and authorization of change requests; establishing separate libraries or directories for development, test, and production source code; and ensuring these directories are properly secured. Controls over changes to data files may include assessing the criticality or sensitivity of the data files, establishing appropriate policies and procedures to handle data changes and emergency change management processes, authorization of changes, and logging and monitoring changes. Controls over changes to system and program files appear to be addressed briefly in the most recent MiSDU SAS 70 report. Controls over changes to data files do not appear to be addressed in the most recent report.

Computer Operations:
Computer operations controls may include organizational segregation of duties, appropriate staffing and job descriptions, and appropriate policies and procedures for job scheduling, equipment maintenance, system maintenance, and data maintenance that is handled by computer operations staff. Controls over the computer operations functions do not appear to be covered in the most recent MiSDU SAS 70 report.

Based on our review, we concluded that the MiSDU SAS 70 Report appears to provide adequate coverage of the business process control environment and activities, but does not provide adequate coverage of the information system processing control environment and activities. Addressing these recommendations in the next annual MiSDU SAS 70 Report would strengthen the usefulness of the report and would help provide FIA assurance that the 3rd party vendor's controls at the MiSDU are in place and functioning adequately. The Office of Internal Audit is available for consultation regarding questions concerning these recommendations.

c: Marilyn Stephen